Image Forgery Detection

PROJECT REPORT

Submitted for the course
CSE3999-Technical Answers to Real World Problems (TARP)

by

NAME	REG NO
Kushagra Singh	18BCE0017
Pavan Siddharth	18BCE0044
Adhil Mohammed	18BCE0056
Ramachandran R	18BCE2508

Slot: TD2

Name of faculty: Dr. K. Jayakumar

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

May, 2021

CERTIFICATE

This is to certify that the project work entitled "**Image Forgery Detection**" that is being submitted by "**Kushagra Singh 18BCE0017, Pavan Siddharth 18BCE0044, Adhil Mohammed 18BCE0056, Ramachandran R 18BCE2508**" for CSE3999 Technical Answers to Real World Problems (TARP) is a record of bonafide work done under my supervision. The contents of this Project work, in full or in parts, have neither been taken from any other source nor have been submitted for any other CAL course.

Place: Vellore

Date: 30 May 2021

Signature of Students:

Kushagra Singh

Pavan Siddharth

Adhil Mohammed

Ramachandran R

ACKNOWLEDGEMENTS

I take immense pleasure in thanking **Dr. G. Viswanathan**, my beloved Chancellor, VIT University and respected Dean, **Dr. K. Ramesh Babu**, for having permitted me to carry out the project.

I express gratitude to my guide, **Dr. K. Jayakumar**, for guidance and suggestions that helped me to complete the project on time. Words are inadequate to express my gratitude to the faculty and staff members who encouraged and supported me during the project. Finally, I would like to thank my ever-loving parents for their blessings and my friends for their timely help and support.

Signature of Student
Adhil Mohammed
Kushagra Singh
Pavan Siddharth
Ramachandran R

Executive Summary

We have developed a website that allows users to upload an image and the website will tell the user if the image has been doctored and also show the parts of the image that have been modified. We have used the images from the CASIA dataset to train our machine learning model. We take the images from the CASIA dataset and perform preprocessing to obtain the types of manipulations, bounding box coordinates and ground truth mask for training the model. Bounding box is found from the ground truth mask. The dataset contains class labels as “Authentic” or “Tampered” which helps in training the classification model. A fully convolutional neural network will be developed which will be able to handle images of different dimensions along with identifying different types of known forgery types like copy-move, splicing, removal, enhancement, and other types. The network consists of two parts: first is the image manipulation trace feature extractor, and second is the local anomaly detection network. After the image has been uploaded to the website, it will be tested by the Neural Network which will then generate the results that shows parts of the image that have been tampered in white while the original parts will remain black i.e. a mask will be presented to the user. In order to test the input image on the website, the neural network model will be integrated with the website in the backend.

CONTENTS

List of Figures

List of Tables

List of Abbreviations

CNN	Convolutional Neural Networks
AI	Artificial Intelligence
LSTM	Long Short Term Memory
JPEG	Joint Photographic Experts Group
ELA	Error Level Analysis

1. INTRODUCTION

Social media plays a significant role in the everyday lives of people in this technological age. There has been a huge increase in the amount of image data generated in the last decade with the advent of social networking sites such as Facebook and Instagram. For social network-based companies such as Facebook, the use of the image (and video) editing tools such as GNU Gimp, Adobe Photoshop to produce doctored images and videos is a major concern. Such pictures are primary sources of false news and are also used for crowd incitement in malevolent ways. Most people frequently post messages, photographs, and videos on social media (e.g. Twitter, Snapchat, Facebook, and Instagram). Photos are one of the most prevalent ways of media sharing on social media among users. Therefore, the monitoring of images found in social media is important. It has now become possible for individuals and small communities to create and widely disseminate these photos in a very short period, threatening the credibility of the news and public confidence in the means of social communication. Also, due to the large increase in population size, nowadays ID proofs like the Aadhaar card, Voter ID, etc. are verified automatedly. This may increase the possibility of submission of fake/doctored ID proofs and get approval. Likewise, forged images can also be submitted in court as proof. This may lead to the punishment of an innocent person or a guilty person may escape from punishment.

1.1. OBJECTIVE

In this project, deep learning will be used to predict if an image is manipulated or not and the parts of the image where any kind of manipulation has been performed will be shown. The kind of manipulation will also be provided as an output along with the mask of tampered parts.

1.2. MOTIVATION

Through this project the problem of detecting image forgery on digital images will be solved which is used to spread false news on social media platforms, used in manipulation of documents, manipulation of identity proofs which can lead to identity theft, etc. Detection of false news on social media platforms allows the administrators to take quick action by removing the particular image from spreading further. Using it in the court of law helps in identifying if people are submitting valid proofs or not. The benefits of integrating such an application in different places in our society has been the motivation to develop this project.

1.3. BACKGROUND STUDY

In the field of image forensics, there are many types of manipulations like copy-move, splicing, removal etc. Over the years many methods have been proposed to detect manipulations. Before the rise of neural networks, researchers were trying to utilize the JPEG compression algorithm [1,2,8,9,10] to detect whether an image is manipulated or not. One such method is error level analysis [1]. But this method would work only on JPEG images and was able to detect only one or two types of manipulations. After neural networks became popular the accuracy of binary classification of whether an image is tampered or not, increased. Researchers started exploring whether they could classify what type of manipulations have been done on the image. In [3] Bayar et.al proposed a convolutional filter which could detect all kinds of manipulations. In [5] Bappy et.al proposed a Conv LSTM model to localize which parts of the image have been forged. In [4] Zhou et.al proposed a faster R-CNN network to detect all kinds of manipulation. They also proposed a noise model using a spatial rich model filter which also localizes which parts of the image have been forged. In [21] Yang et.al proposed a model similar to [4] using masked R-CNN to classify the manipulation as well as localize the forged part.

The authors of [11] have proposed a methodology which performs detection of splicing and copy-move forgery at the same time using the statistical properties of the AC components of the block DCT coefficients and the changes that occur in them. In [12], methodology proposed uses a combination of splice detection using the compression level of JPEG images followed by the Error-Level analysis technique highlighting the pixels that have a different compression level than the rest of the image. These parts are then marked. The algorithm proposed in [13] integrates Fast Fourier Transforms with local texture descriptors for detecting image forgery. It uses existing block-based methodology. [14] have proposed using clustering algorithms which will help in increasing the block matching strategy speed. Block level analysis using DCT is followed by the K Means algorithm for the clustering. The methodology proposed in [15] uses super-pixel segmentation and Helmert transformation. Matching pairs are obtained and then localized. An algorithm based on multi-scale analysis was proposed in [16]. The image is voted on a multi-scale basis and analysis of the generated groups using a descriptor that is highly resistant to rotation, scaling, and compression is done, reducing the search space for duplicated regions and yielding a detection map. The authors of [17] have worked on forgery detection using Gabor magnitude. After appropriate post-processing, feature vectors are lexicographically sorted, and duplicated image blocks are detected by identifying

resemblance block pairs. [18] have used intrinsic resampling properties for fast forgery detection. Another paper [19] has put forward a method for image resampling detection. Resampling detection features are learned adaptively and directly from data using a constrained convolutional layer. [20] proposed a new method using various JPEG compression and Gaussian noise and blurring attacks, for detecting copy-move forgery in images. Feature extraction, feature matching, and duplicate block recognition are all part of the process. The authors of [22] have worked on only copy-move image forgery as it is the most common type of forgery and is very easy to forge. The proposed method involves using the Gaussian-Hermite moments. The RANSAC algorithm is used to filter the outliers from the inliers by taking into account scaling. The evaluation is done at both the pixel-level and the image-level.

2. LITERATURE SURVEY

S. No.	Paper Title	Methodology	Needed Improvements	Future work
Image Forgery Detection				
1	Image forgery detection using error level analysis and deep learning [1]	In this paper, the author implements a fake image detection using Error level analysis and VGG 16 CNN model. ELA is a technique which saves the JPEG image and compares the difference of pixel values of the saved image with the initial image. The training is done with CASIA v2 dataset.	The accuracy came out to be 88.16%.	Works only with JPEG images. When an image is saved many times then the difference between pixel values will be small. The method will be ineffective. Only image classification is done. Image localization is not done.

2	A deep learning approach to detection of splicing and copy-move forgeries in images [2]	In this paper, the author proposed a 10-layer CNN model to detect photoshopped images. The simple high-pass filter collection used in the computation of residual maps in the spatial rich model (SRM) is used to initialise the weights at the first layer of our network, which serves as a regularizer to efficiently suppress the influence of image contents and collect the subtle objects introduced by the tampering operations.	The accuracy has been checked with 3 datasets: CASIA v1, CASIA v2 and DVMM. The model had an accuracy of 98.04%, 97.83% and 96.38 respectively.	This model works only for copy-move and image-splicing manipulations. Work for other manipulations can be done. This model only does forgery classification. Work on forgery localization can be done.
3	A Deep Learning Approach To Universal Image Manipulation Detection Using A New Convolutional Layer [3]	In this paper, the authors developed a new form of convolution layer that can learn image manipulation features. It can learn and detect many forms of image manipulation and not just one or two. They used their own created dataset.	The accuracy for the CNN model is 99.31%.	Only image forgery classification for grayscale images is done. Could be extended to RGB images also. Image localization is not done.

4	Learning Rich Features for Image Manipulation Detection [4]	This paper proposed a two-stream R-CNN network to detect the tampered regions of the manipulated image. One of the two streams is an RGB stream whose purpose is to extract features from the RGB image to find visual tampering features. The other is a noise stream that seeks differences between initial and tampered regions by using noise features derived from a steganalysis rich model filter layer.	The accuracy was checked with 4 datasets: NIST, Columbia, COVERAGE and CASIA. It came out to be 93.7% 85.8% 81.7% 79.5% respectively.	The accuracy for copy-move manipulation could be improved.
5	Exploiting spatial structure for localizing manipulated image regions [5]	This paper focuses on localizing the parts of the image that are manipulated. They proposed a CNN-LSTM model. This paper finds the manipulated parts for various types of manipulation techniques and different image formats. The evaluation of the model is done in two stages: Patch	The accuracy is checked with 3 datasets: NIST, IEEE Forensics Challenge and COVERAGE. For patch classification it had accuracy of 89:38%, 87:68% and 80:06% respectively and for segmentation it had accuracy of 84:60%, 77:67% and 81:14% respectively.	The accuracy of the model should be improved although it performed very well compared to existing models.

		Classification and segmentation of manipulated images.		
6	A Robust Forgery Detection Method for Copy–Move and Splicing Attacks in Images [6]	This paper uses the FBDDF dataset and an SVM classifier (LIBSVM) for the binary classification model using the radial basis function (RBF) as the SVM kernel. Ten-fold cross validation is used to divide the dataset into training and test sets and to improve the model.	Accuracy of the model is bad when the images are in uncompressed format.	When the image is distorted the model does not perform well. So the model has to consider images where there's barrel distortion like the ones captured by fisheye wide-angle lenses.
7	Digital Image Forgery Detection [7]	They have created their own dataset and a naïve-bayes classifier is used for classification. Blocks of images , either overlapping or non-overlapping are fed to the model instead of images as a whole. Image analysis, texture analysis and pixel value analysis are used to extract features.	The accuracy of the method drops when the forgery technique involved is image retouching.	Hybrid machine learning models can be used for better results.

8	Pixel based Image Forensic Technique for copy-move forgery detection using Auto Color Correlogram [8]	The images used in the dataset are processed by filtering noise and then divided into blocks. Auto color correlogram of each block is used to extract features. To compute the mean colour, ACC takes into account all the pixels of Colour Cj at a specific distance from all the pixels of Colour Ci. Manhattan distance is used as the similarity measure to find the match and detect forgery.	The model is not able to detect multiple forgeries in the same image.	Adding images with various transformations like scaling and distortion to the dataset will improve the accuracy of the model.

9	Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies [9]	JPEG compression of an image introduces vertical and horizontal breaks called block artificial grids (BAG) . If the picture is intact, these breaks should only appear on block borders. However if the image is modified, these breaks start appearing within the image. This paper uses this method and detects forgery by performing calculations with the pixel values to determine the presence of BAGs within the borders.	The model does not detect forgery in images where there is very less or no compression.	Techniques other than just copy-move and splicing need to be detected by the model.

10	An efficient approach for forgery detection in digital images using Hilbert–Huang transform [10]	The first step is converting the RGB image into YCbCr color space. The second step is extracting the HHT (Hilbert–Huang transform) features. The HHT consists of two stages. In the first stage, the signal is decomposed into Intrinsic Mode Functions (IMF) for obtaining the instantaneous frequency information, this means that any complicated dataset decomposes into a finite number of components. In the second stage, Hilbert transform is used for computing the instantaneous frequencies and amplitudes which are used as features for image forgery detection. Then classification is done using SVM, ANN and KNN and then the results are compared.	The accuracy of the model decreases with the increase in image quality.	Improving the detection rate in the presence of attacks by using and optimizing another verification parameter such as the cross correlation

11	Image forgery detection based on statistical features of block DCT coefficients [11]	In the paper, the authors have proposed a methodology which performs detection of splicing and copy-move forgery at the same time. When a JPEG image is tampered, the statistical properties of the AC components of the block DCT coefficients change. The image is then cropped and the suggested features are extracted for the test image and the cropped version of the image. The support vector machine (SVM) is used to distinguish genuine and forged images using the derived attribute vector.	Since the algorithm uses SVM to classify the images, the main disadvantage turns out to be the execution time, especially when a large dataset is being used to train the model.	The execution time of the classification algorithm needs to be improved to increase the efficiency.

12	Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression [12]	The authors have proposed two algorithms for detecting image forgery. The first algorithm uses splice detection using the compression level of JPEG images. The Error-Level analysis technique highlights the pixels that have a different compression level than the rest of the image. These parts are then marked. The second algorithm uses Colour Filter Array detection technique. First, the interpolation pattern of the colour filter matrix of the digital camera that captured the image is estimated. The image is then re-interpolated with different CFA patterns. The Mean Square Error for each pattern is obtained between the original and re-interpolated image. The results obtained here are analysed to determine whether	The proposed algorithms are not suitable to detect modifications in images that are having smaller dimensions (e.g., 700x700 pixels). Images that have big white areas end up giving false positives which reduces the accuracy.	The algorithm needs to be improved in order to work for smaller images which will also increase the accuracy.

		the image was modified or not.		
13	Detection of Digital Image Forgery using Fast Fourier Transform and Local Features [13]	The algorithm proposed in this paper integrates Fast Fourier Transforms with local texture descriptors for detecting image forgery. It uses existing block-based methodology. First, the image matrix is transformed into its discrete fourier coefficients. It is then segmented into overlapping blocks. Then, Enhanced Local Ternary Pattern (ELTP) is used on the blocks to obtain the feature vectors. The feature vector contains ELTP code for every FFT block of the image. These feature vectors are fed to the SVM classifier to get the results as forged or authentic.	Both of the approaches presented by the authors involve complex transformations like Discrete Cosine Transform and Fast Fourier Transform which increases the time complexity of the methodology. Also, the forged parts of the image are not localized and marked.	Identification of forged parts is needed. Time complexity can also be reduced.

14	Block-based copy–move image forgery detection using DCT [14]	The authors have proposed using clustering algorithms which will help in increasing the block matching strategy speed. The image is first converted to grayscale, then it is further divided into overlapping blocks of size 8x8. DCT is used to extract the features on the basis of different feature sets. Block clustering is done using the K-Means algorithm. Finally, radix sort is used for feature matching.	Overlapping the blocks of the image plays a huge part in this algorithm. But, as the size of the blocks is increased, the speed of the algorithm increases but at the cost of failure in detection of the forged parts.	A balance needs to be found by choosing an appropriate block size which will then give efficient results with good accuracy.
15	Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation [15]	First, a scale-invariant feature transform is used to extract the keypoints and descriptors. Matching pairs are obtained by calculating the similarity between descriptors and keypoints. The matching pairs are grouped based on the spatial distance with the help of Helmert transformation and	The execution time of the proposed algorithm is higher than most of the commonly used algorithms. The proposed method is also not robust against detecting tampered parts that are symmetric, recurring or smooth patterns.	The execution time needs to be reduced along with improvements in being able to detect smooth or symmetric patterns.

		obtain the coarse forgery regions. These regions can then be localized.		
16	Going deeper into copy-move forgery detection: Exploring image tell-tales via multi-scale analysis and voting processes [16]	A digital image was analysed and voted on a multi-scale basis. Extract interest points that are immune to scale and rotation from a suspicious image and search for potential correspondences. Then, using geometric constraints, organise the correspondent points into regions. Then, for each scale, analyse the generated groups using a descriptor that is highly resistant to rotation, scaling, and compression, reducing the search space for duplicated regions and yielding a detection map. A voting process among all detection maps determines the final decision.	It's likely that the detector won't locate enough key points in a small or homogeneous area, allowing it to be discarded or blocked from further evaluations. Also this supports only JPEG format images.	To do with far more complicated processes when they're mixed (e.g., blurring, different noise addition, etc.). New techniques for describing block pixels and other methods for detecting representative key points are also possible enhancements.

17	Copy-move image forgery detection based on Gabor magnitude [17]	The tampered picture is first segmented into overlapping fixed-size blocks, with each block receiving the Gabor filter. As a result, each block is represented by a Gabor magnitude graphic. Second, from the histogram of oriented Gabor magnitude (HOGM) of overlapping blocks, statistical features are extracted and reduced features are produced for similarity calculation. After appropriate post-processing, feature vectors are lexicographically sorted, and duplicated image blocks are detected by identifying resemblance block pairs.	Image manipulation can be hidden using more sophisticated techniques like great rotation, scaling, noise incorporation, inpainting, or a mixture of these. This makes detecting copy-move forgery even more difficult. These needs to be improved.	Uses JPEG formatted images. So, it should be re-configured such that other format images also can be taken into account for input.

18	Fast Forgery Detection with the Intrinsic Resampling Properties [18]	Using the pre-calculated resampling weighting table and the periodic properties of the projection error distribution, depending on the intrinsic properties of the resampling scheme to detect the tampered regions.	However, the detection accuracy of this method is about 95% and the time taken for detecting a 512×512 image needs around 50 seconds.	Time complexity of the algorithm to be reduced and the error projects should be decreased.
19	On the robustness of constrained convolutional neural networks to JPEG post-compressio n for image resampling detection [19]	Adaptively learn resampling detection features directly from data using a constrained convolutional layer. In this study, CNN was used as a binary classifier to detect resampling operations in re-compressed images with various scaling factors and JPEG compression consistency factors. Furthermore, CNN used deep convolutional features to train an extremely randomised trees (ET) classifier.	Typically to achieve an accuracy higher than 91.22% with all the quality factors except for 120% upscaled images with QF=50 which are detected with an accuracy equal to 84.08%. Though the detection accuracy decreases when using a low post-compression quality factor.	The accuracy of the model needs to be improved for both upscaled and downscaled images.

20	Robustness of copy-move forgery detection under high JPEG compression artifacts [20]	Under various JPEG compression and Gaussian noise and blurring attacks, a method for detecting copy-move forgery in images has been developed. Feature extraction, feature matching, and duplicate block recognition are all part of the process. For feature extraction, the fast Fourier transform (FFT), singular value decomposition (SVD), and principal component analysis (PCA) are used. Then, for function matching, FFT, SVD, and PCA cascading matchers are used. Cascade filtering with city block, lateral, vertical, and frequency filters is used to classify matched blocks. Finally, the pixels in the upper left corners of duplicate blocks that have been observed are outputted for visual analysis.	To achieve a suitable solution, tuning too many parameters is intractable and time-consuming. This is the primary motivation for proposing a threshold-free algorithm to prevent such tuning work, but it ultimately increases the proposed framework's time and configuration complexity.	Cannot accurately Identify the doctored parts in the image and also execution time needs to be reduced.

21	Constrained R-CNN: A general image manipulation detection model [21]	This paper proposes an architecture with the following layers for manipulation detection: The learnable manipulation feature extractor (LMFE) .Instead of predetermined features, this layer analyses the content manipulation directly from the data and represents them as features. The constrained R-CNN layer which classifies the manipulation techniques and performs image segmentation to highlight the manipulated regions simultaneously. An attention regional proposal network (RPN-A) to discriminate the manipulated regions effectively.	The F1 scores of the model are low when tested on the CASIA dataset as compared to the other benchmark datasets.	The model needs to outperform the RGB-N model on splicing detection.

3. PROPOSED SYSTEM

3.1. ANALYSIS AND DESIGN

The aim of the proposed system is to detect if an image is tampered or not, and detect the regions of tampering, if any. This is done by first taking an input image and uploading it to the website. The website submits the input image to the backend where the trained convolutional neural network is present. The CNN model is trained by passing tampered images as the input and the ground truth mask as the output. The model applies various filters based on the layers added to predict the mask. In each iteration, the loss value is calculated which is back propagated to update the filters. The trained model is saved to be used in the website backend.

The image is passed into the model in order to get the output mask which marks the tampered regions in a lighter colour. After processing, the input image and the predicted mask are displayed back to the user on the website.

The proposed system consists of a website to upload tampered images and display the output, a CNN model that localises the regions of tampering, and a python backend that connects the website to the CNN model.

3.2. ARCHITECTURE/FLOWCHART

a. Neural Network

A deep neural network which will show the localized mask of the manipulated region. It first extracts image manipulation trace features for a testing image, and identifies anomalous regions by assessing how different a local feature is from its reference features. There are 2 networks here: the image manipulation trace feature extractor and deep anomaly detection.

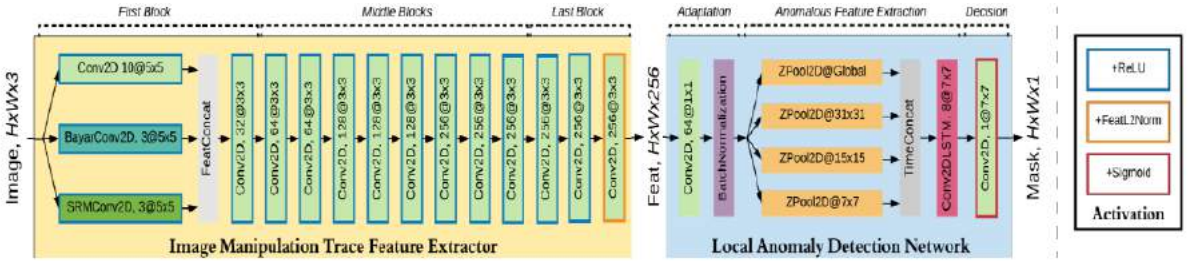


Fig. 1. Architecture of the Convolutional Neural Network

The backbone of the architecture is the VGG-16 network. An inception network is created with 3 different convolutional filters. The inception stack is then passed onto this VGG-16 network. Then we apply a 1x1 convolution filter and then apply Z-pooling. This is passed onto the ConvLSTM network.

b. Application Architecture

A website where users can upload an image. This image will be passed through the neural network and will check if that image has been manipulated or not.

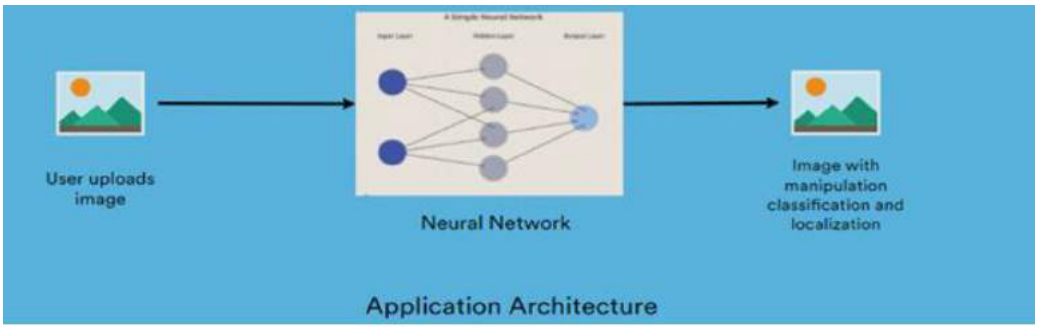


Fig. 2. Application Architecture

c. Workflow Diagram

The workflow diagram below divides the entire project into separate modules which are being worked upon and are then combined to get the final results.

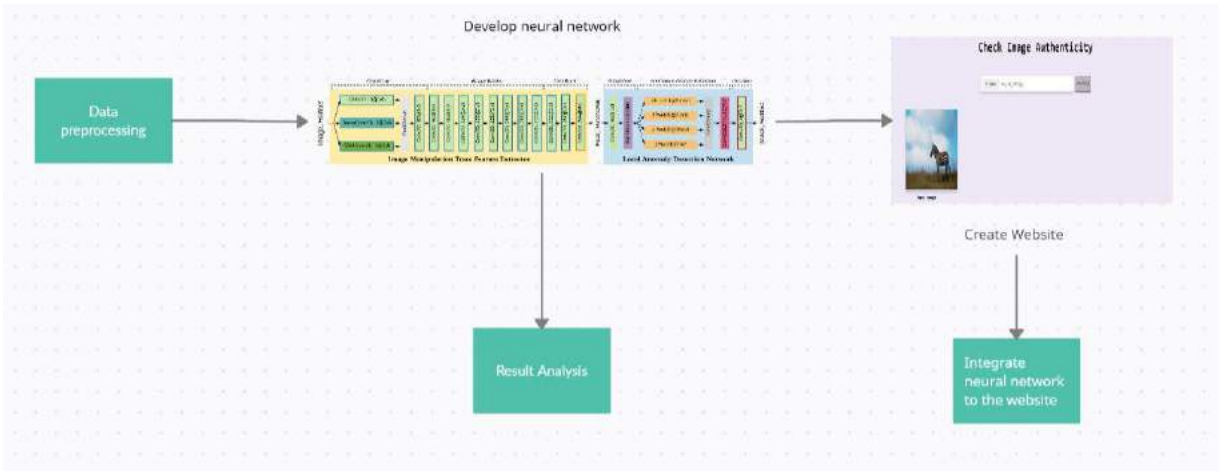


Fig. 3. Workflow Diagram

3.3. MODULE DESCRIPTION

a. Data Preprocessing

In this module, we take the images from the CASIA dataset and perform pre-processing to obtain the types of manipulations, bounding box coordinates and ground truth mask for training the model. Bounding box is found from the ground truth mask. The dataset contains class labels as “Authentic” or “Tampered” which helps in training the classification model.

Pseudocode:

For each image:

Read AuthenticImage

Read TamperedImage

Convert both images to grayscale

Mask = AuthenticImage – TamperedImage

Save the generated mask

Generate contour for the mask

Save the contour

Generate bounding box coordinates for each image

End For

b. Neural Network

Here, a fully convolutional neural network will be developed which will be able to handle images of different dimensions along with identifying different types of known forgery types like copy-move, splicing, removal, enhancement, and other types. The network consists of two parts: first is the image manipulation trace feature extractor, and second is the local anomaly detection network.

Pseudocode:

- Create Bayar Convolutional layer
- Create SRM Convolutional Layer
- Create Conv2D layer with 5x5x10 filter
- Concatenate all the 3 outputs
- Create 10 Convolution layers with ReLU Activation function
- Perform 1x1 Convolution on output of previous step
- Perform BatchNormalization
- Perform ZPooling and pass the output to Conv2DLSTM layer.
- Perform 1x1x7 Convolution

c. Website to Check for Forgery

In this module, firstly, a website will be developed which will enable the users to upload an image from their local computers to the website. After the image has been uploaded, it will be

tested by the Neural Network which will then generate the results that shows parts of the image that have been tampered in white while the original parts will remain black i.e., a mask will be presented to the user. In order to test the input image on the website, the neural network model will be integrated with the website in the backend.

4. TECHNICAL SPECIFICATION

Hardware Requirements:

- Intel i7 Processor
- 8 GB RAM or higher
- Minimum 20 GB of storage space

Software Requirements:

- Python 3.6 or higher
- TensorFlow 1.8
- Keras 2.2
- Jupyter Notebook
- Flask

5. RESULTS AND DISCUSSION

The pre-processing was performed successfully on the CASIA dataset and the ground truth mask was generated and saved for each pair of original and tampered images. After pre-processing, the CNN model was trained to detect image forgery. The tampered image and the corresponding ground truth masks were used to train the model. The layers that were added to the model made sure that the dimensions of the input and output image remain the same.

5.1 Pre-Processing Results

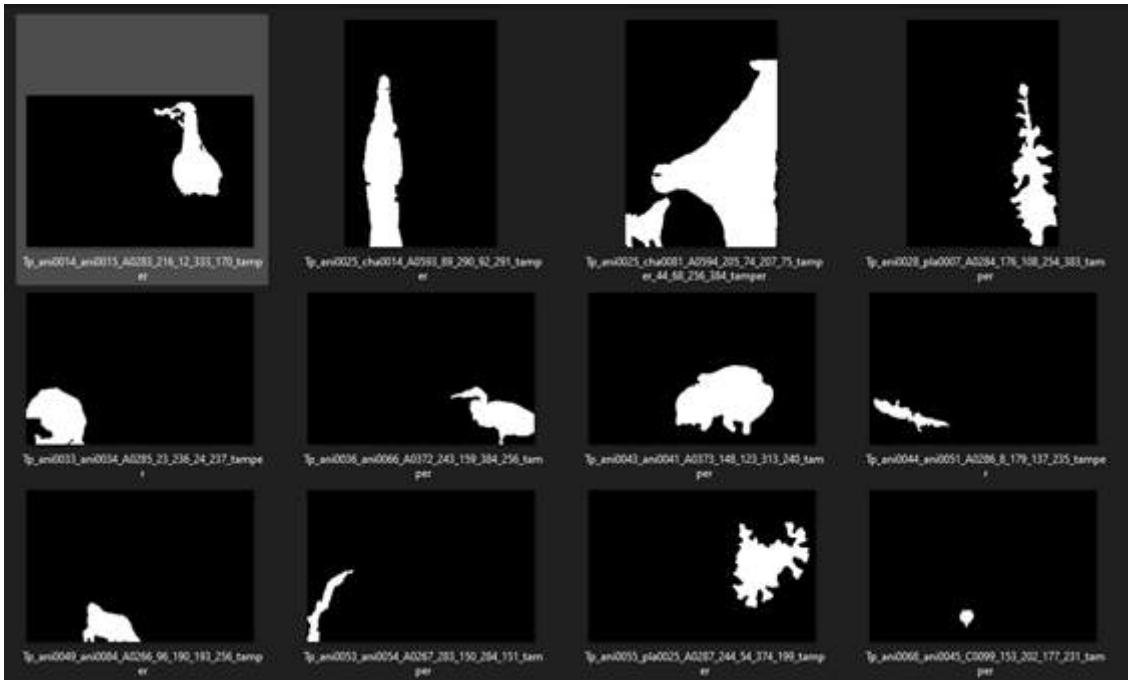


Fig. 4. Ground Truth Masks obtained from Pre-processing the CASIA Dataset

5.2 Comparison of Tampered Image with the Actual Ground Truth Mask

Fig. 5. Comparison of a Tampered Image(left) with the mask of same image(right)

5.3 Predicted Results from the CNN

The following results were obtained by testing different tampered images taken from the CASIA dataset.

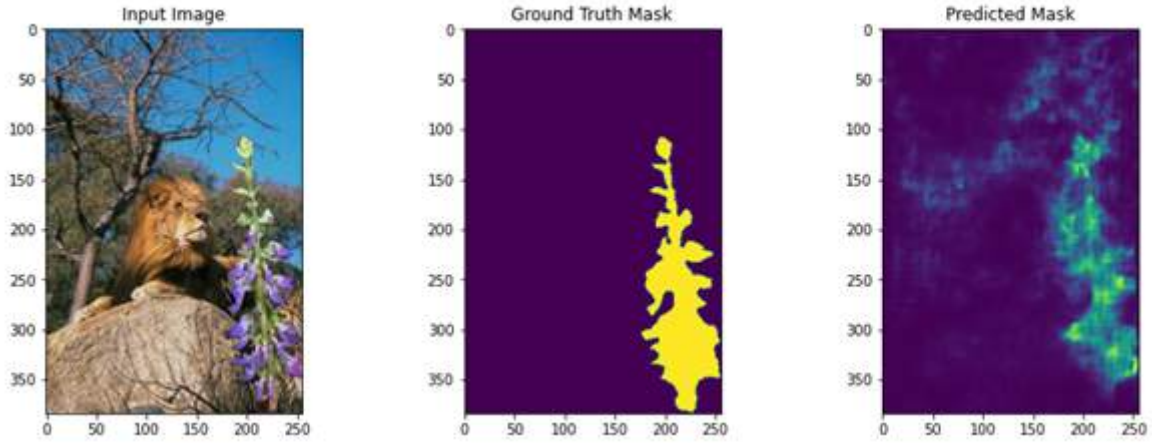


Fig. 6. Test Results for Input Image 1

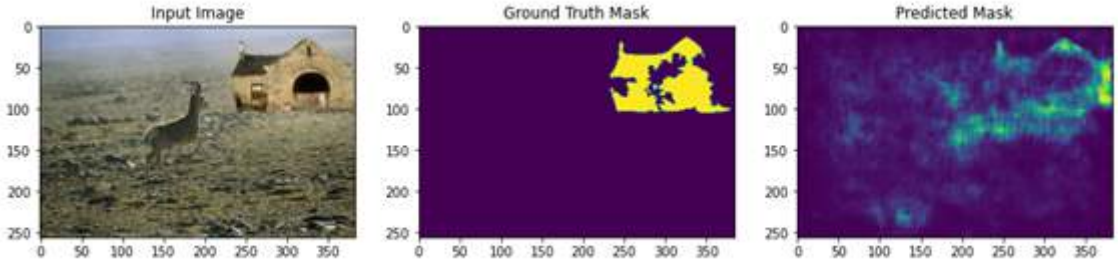


Fig. 7. Test Results for Input Image 2

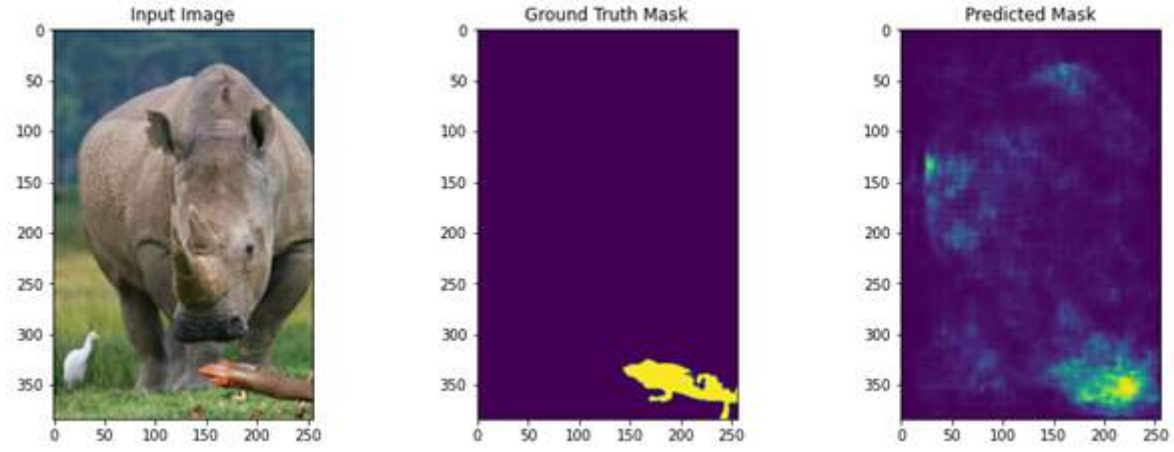


Fig. 8. Test Results for Input Image 3

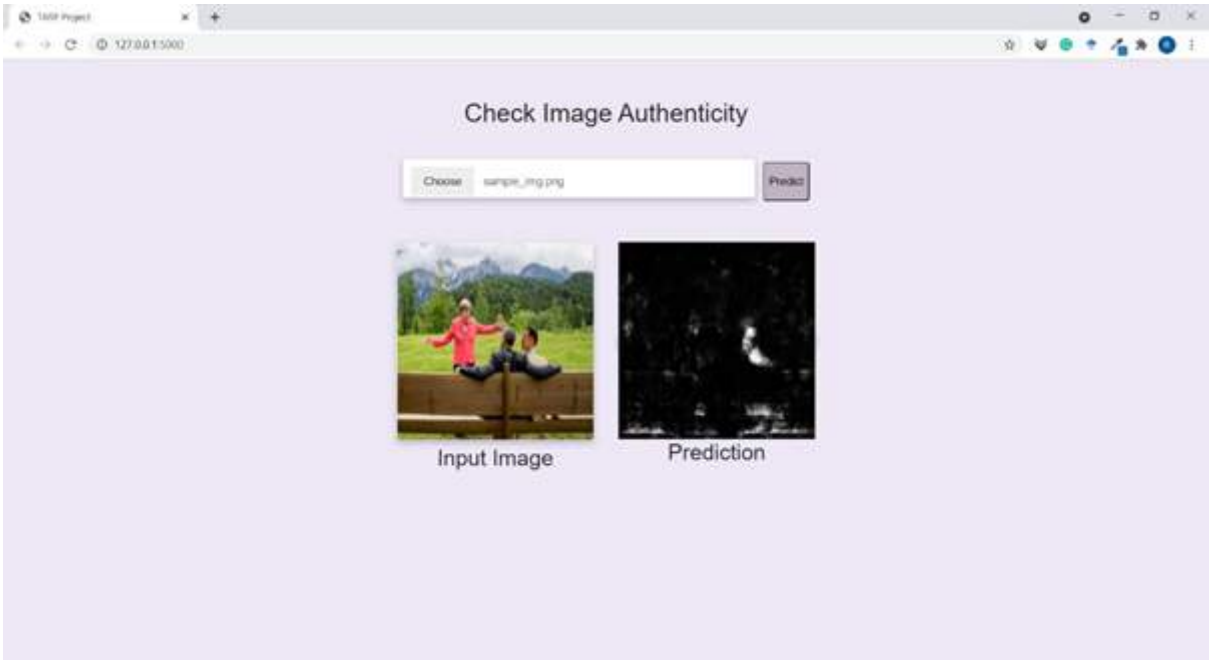
5.4 Accuracy and F1-Score

The accuracy and the F1-score are calculated by comparing the ground truth masks with the predicted masks. These results are obtained by comparing both the images pixel-wise to see if the pixel is classified correctly or not. The comparisons are done after applying image thresholding to the predicted mask in order to get better results. On the CASIA dataset, we obtained an accuracy of approximately 88.5% while the F1-score came out to be 0.33. These were the best results that we obtained by applying different thresholds to the predicted mask.

METHODS	**AUC %**	**F1-Score**
ELA	61.3	21.4
EOI1	61.2	26.3
CFA1	52.2	20.7
RGBN	79.5	40.8
Ours	**65.5**	**33.1**

Table 2: AUC and F1 Comparison Table

Image 1 (Splicing Manipulation)



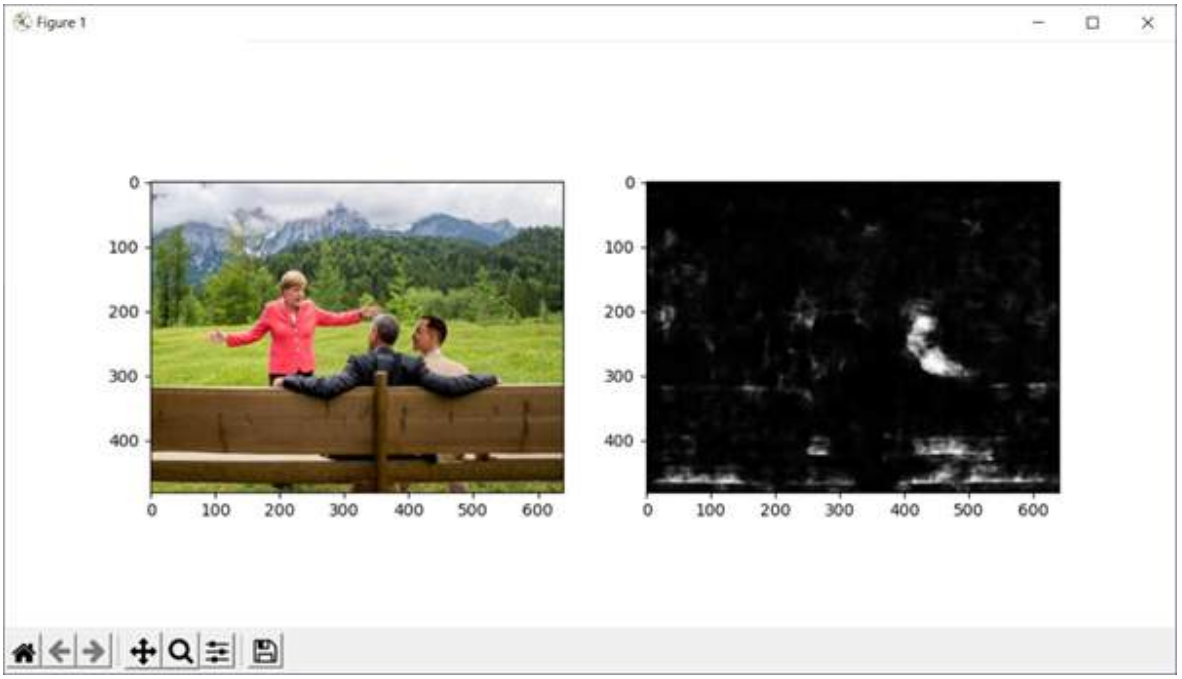
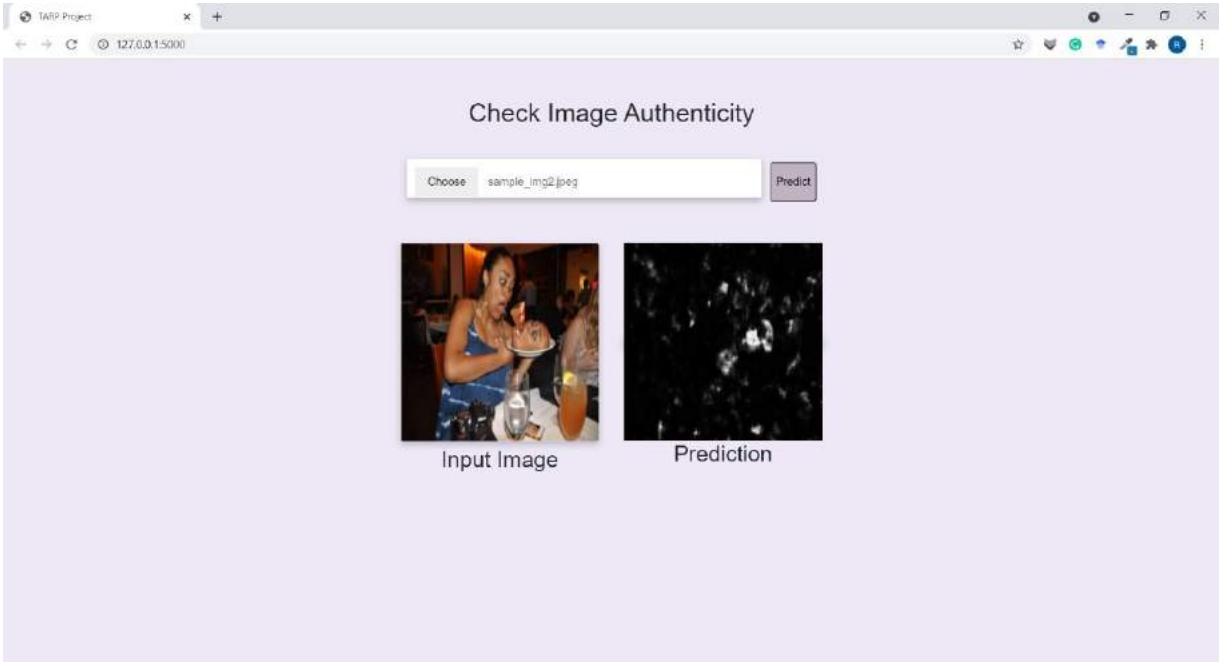
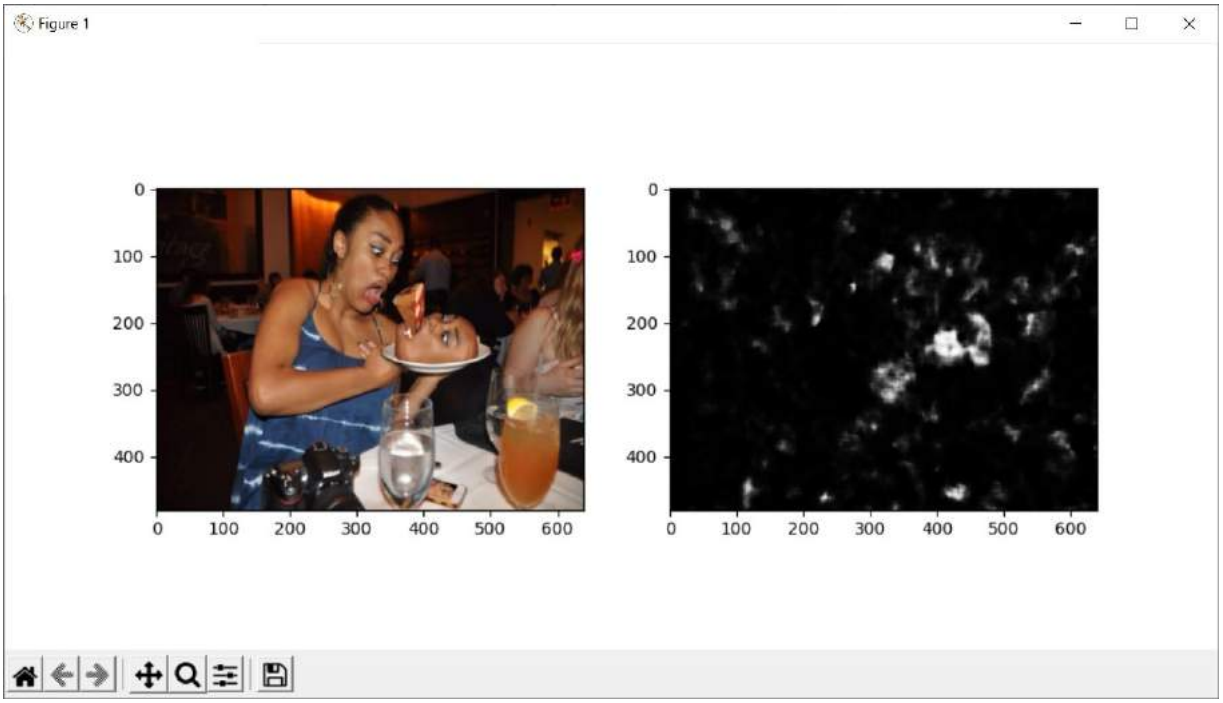


Image 2 (Copy-Move Manipulation)





6. CONCLUSION AND FUTURE WORK

In this project, we have used the deep-learning method of Convolutional Neural Networks to train a model that can detect and highlight the areas of an image that are forged. These forgeries can belong to different classes and the model is trained to detect all of them. The model applies various filters to the base image in order to apply manipulations that can generate the desired output mask highlighting the regions of forgery. The experimental tests

were performed on the CASIA dataset which is a commonly used dataset for detecting image forgeries. The model marks the forged parts in a brighter colour while the original parts remain dark. Along with this, the mask of an image with dimensions 384x256 can be generated within 7-8 seconds. The performance can be drastically improved if GPU support is enabled when using the TensorFlow library as GPUs have a higher memory bandwidth and number of cores, but consume a lot more power than CPUs. This will further allow the model to be trained on new datasets and calculating the accuracies of the models.

References

[1] Sudiatmika, I. B. K., & Rahman, F. (2019). Image forgery detection using error level analysis and deep learning. Telkomnika, 17(2), 653-659.

[2] Rao, Y., & Ni, J. (2016, December). A deep learning approach to detection of splicing and copy-move forgeries in images. In 2016 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6). IEEE.

[3] Bayar, B., & Stamm, M. C. (2016, June). A deep learning approach to universal image manipulation detection using a new convolutional layer. In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security (pp. 5-10).

[4] Zhou, P., Han, X., Morariu, V. I., & Davis, L. S. (2018). Learning rich features for image manipulation detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1053-1061).

[5] Bappy, J. H., Roy-Chowdhury, A. K., Bunk, J., Nataraj, L., & Manjunath, B. S. (2017). Exploiting spatial structure for localizing manipulated image regions. In Proceedings of the IEEE international conference on computer vision (pp. 4970-4979).

[6] Islam, M. M., Karmakar, G., Kamruzzaman, J., & Murshed, M. (2020). A Robust Forgery Detection Method for Copy–Move and Splicing Attacks in Images. Electronics, 9(9), 1500.

[7] Shyry, S. P., Meka, S., & Moganti, M. (2019). Digital Image Forgery Detection. International Journal of Recent Technology and Engineering (IJRTE), 8.

[8] Malviya, A. V., & Ladhake, S. A. (2016). Pixel based image forensic technique for copy-move forgery detection using auto color correlogram. Procedia Computer Science, 79, 383-390.

[9] Liu, B., Pun, C. M., & Yuan, X. C. (2014). Digital image forgery detection using JPEG features and local noise discrepancies. The Scientific World Journal, 2014.

[10] Kasban, H., & Nassar, S. (2020). An efficient approach for forgery detection in digital images using Hilbert–Huang transform. Applied Soft Computing, 97, 106728.

[11] Dua, S., Singh, J., & Parthasarathy, H. (2020). Image forgery detection based on statistical features of block DCT coefficients. Procedia Computer Science, 171, 369-378.

[12] Vega, E. A. A., Fernández, E. G., Orozco, A. L. S., & Villalba, L. J. G. (2020). Passive image forgery detection based on the demosaicing algorithm and jpeg compression. IEEE Access, 8, 11815-11823.

[13] Kanwal, N., Girdhar, A., Kaur, L., & Bhullar, J. S. (2019, April). Detection of digital image forgery using fast fourier transform and local features. In 2019 International Conference on Automation, Computational and Technology Management (ICACTM) (pp. 262-267). IEEE.

[14] Parveen, A., Khan, Z. H., & Ahmad, S. N. (2019). Block-based copy–move image forgery detection using DCT. Iran Journal of Computer Science, 2(2), 89-99.

[15] Huang, H. Y., & Ciou, A. J. (2019). Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. EURASIP Journal on Image and Video Processing, 2019(1), 1-16.

[16] Silva, E., Carvalho, T., Ferreira, A., & Rocha, A. (2015). Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. Journal of Visual Communication and Image Representation, 29, 16-32.

[17] Lee, J. C. (2015). Copy-move image forgery detection based on Gabor magnitude. Journal of Visual Communication and Image Representation, 31, 320-334.

[18] Lien, C. C., Shih, C. L., & Chou, C. H. (2010, October). Fast forgery detection with the intrinsic resampling properties. In 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 232-235). IEEE.

[19] Bayar, B., & Stamm, M. C. (2017, March). On the robustness of constrained convolutional neural networks to jpeg post-compression for image resampling detection. In 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 2152-2156). IEEE.

[20] Huang, D. Y., Huang, C. N., Hu, W. C., & Chou, C. H. (2017). Robustness of copy-move forgery detection under high JPEG compression artifacts. Multimedia Tools and Applications, 76(1), 1509-1530.

[21] Yang, C., Li, H., Lin, F., Jiang, B., & Zhao, H. (2020, July). Constrained R-CNN: A general image manipulation detection model. In 2020 IEEE International Conference on Multimedia and Expo (ICME) (pp. 1-6). IEEE.

PAPER PUBLICATION DETAILS

IJEAST Paper id :- 12220 for the Paper Titled Image Forgery Detection for Digital Forensics: A Survey

Inbox ×

editor@ijeast.com Fri, May 28, 5:25 PM (2 days ago)

to me

Dear Adhil Mohammed, Kushagra Singh, Pavan Siddharth, Ramachandran R, Jayakumar K,

Greetings from IJEAST!
We Acknowledge the Receipt of the Paper Submitted in IJEAST. Your PAPER-ID :- 12220, Please keep this id for the Future reference. We will Assign the DOI against this id only We are reviewing your paper and will revert you shortly.

Regards,
Editor In Chief
International Journal of Engineering
Applied Science and Technology

Reply Forward